February 2005

RFID Update

We are providing this document to keep you informed on our latest activities and observations related to RFID technology. Please let us have your comments and feedback.

Thank you,

Peter Winer (peter@bigchief.com)

Alice Lankester (alice@bigchief.com)

Chris Meisl (chris@bigchief.com)

In This Issue:

Recent Activities at Big Chief Partners

Since our last newsletter in November 2004, we have diversified our activities. In addition to RFID, we have also been involved in security, Web strategy and product management.

In RFID, we are continuing to implement device-handling for **Blue Vector Systems**. Blue Vector Systems provides RFID network infrastructure consisting of appliances and routers that reduce operational complexity and make deployment easier. We have also completed a three month strategic advice project for **Wavetrend**, based in London, U.K., where we provided advice to the company on applications and technology strategy related to their active RFID offerings.

In security, we are continuing to provide implementation and usability advice for **Determina**, a leading provider of host intrusion detection systems. We contributed to the Determina's Enterprise Management Console, used to manage hundreds of protected servers. The company is now gaining market traction, with successful deployments at significant global enterprises.

In Web strategy, we completed an interesting project for semiconductor powerhouse **AMD**, and their subsidiary **Spansion**. The companies needed an outside opinion on how to integrate global web content management systems for AMD, Spansion and Fujitsu in an efficient and effective manner. In a fairly rapid timeline, we were able to assess the options available to the company and make recommendations that met their fiscal and technological goals.

Recently, we have started a new engagement with existing client **BEA Systems**, providing product management for the worldwide launch of BEA's new WebLogic Communications Platform – a product suite aimed at the telecommunications industry. This important launch is the first of the new solutions-focused strategy for BEA Systems.

Events

In October 2004, Peter Winer chaired the **RFID Solutions Conference** in Toronto, Canada. Presenters included IBM, Microsoft, Oracle, ExxonMobil, Home Depot, Procter and Gamble, Marine Terminal Corporation and RCM Technologies. Throughout 2005, Peter will be chairing a series of Canadian RFID events for producer Soft Match.

In November 2004, Peter Winer and Chris Meisl chaired and presented the **RFID Developers Conference** in San Mateo, California. Presenters included Texas Instruments, Sun Microsystems, Oracle, BEA Systems, VivoTech, Odin Technologies, Stockway, Globe Ranger and Connecterra.

Peter and Chris are presenting at **RFID World** in Dallas, Texas, March 1 – 3 2005. We are also working with event producer Shorecliff Communications on several innovative new conferences in 2005. Please let us know if you will be attending RFID World.

RFID Infrastructure Developments

Companies to Watch Infrastructure

IBM
(http://www.ibm.com/rfid)

Intermec
(http://www.intermec.com)

Oat Systems
(http://www.oatsystems.com)

Oracle
(http://www.oracle.com)

SAP
(http://www.sap.com)

Sun Microsystems
(http://www.sun.com/rfid)

Thing Magic
(http://www.thingmagic.com)

ALE Standard

ConnecTerra
(http://www.connecterra.com)

EPC Global
(http://www.epcglobalinc.com)

Globe Ranger
(http://www.globeranger.com)

In recent months, we have seen four notable developments in RFID infrastructure, specifically related to managing information and devices at the network edge.

Application Level Events (ALE) from EPC Global
ALE is a standardized interface between devices that collect RFID data and the systems that consume the data. ALE provides filtering, consolidation and reporting. It also provides separation between physical RFID devices and applications.

IBM's RFID Device Infrastructure
Device Infrastructure is an RFID-enabled middleware product that IBM will make available to partners who will embed it on their devices. Devices that embed this middleware will be able to more efficiently interface with servers running IBM WebSphere software. So far, Intermec is the only major vendor to announce a product that embeds the middleware.

More software vendors with adapters for RFID readers
Sun Microsystems, Oracle and SAP have joined the set of enterprise application and platform vendors who offer adapters that can be used to integrate various RFID readers with their offerings. Globe Ranger and Connecterra – the principal authors of ALE – also offer such adapters.

More companies licensing the Thing Magic Mercury 4 reader
Zebra, Omron and Tyco are all licensing Thing Magic's latest reader and using it in their own branded products. We are also aware of other licensing deals that will be announced in the coming months.

Our Analysis of these Developments

Eighteen months ago – in the second half of 2003 – Savant from EPC Global was the overwhelming focus of attention for RFID middleware. Savant was an evolving specification for collecting and managing the flow of RFID data collected from RFID readers and other devices. Savant was not fully defined and there were no commercial implementations.

Some early adopters - most notably Sun Microsystems – announced that they were implementing Savant. Oat Systems developed the original reference implementation of Savant for EPC Global. They received venture funding and launched themselves as a commercial provider of Savant software for RFID.

Most other industry participants – including us – didn't view Savant as commercial software that would be widely deployed. Instead, we viewed it as a roadmap for defining RFID infrastructure and systems.

Savant never gained mass adoption. In early 2004, EPC Global began to realize that a good part of Savant's value would only be realized when open, multi-vendor deployments managing billions of tags became commonplace. In EPC Global's view, that would imply item-level tagging of consumer goods. Such tagging will not be feasible for at least five years.

As a result, EPC Global switched their focus to ALE in early 2004. ALE was introduced to provide a standard interface between devices, the information they collect and the applications that consume the information. Throughout 2004, EPC Global worked to completely define ALE and we expect the published specification to emerge during the first half of 2005.

At the same time, there has been sustained commercial interest in capitalizing on RFID. So now in early 2005, various companies are leveraging the ideas from ALE in their strategies. With ALE still emerging, credible alternatives are already gaining traction. It is still possible that ALE will gain wide acceptance as a standard interface. It is also possible that the industry will continue progressing without a strong standard. It is even possible that the Thing Magic reader interface will emerge as a de facto standard, based purely on licensing and customer

RFID Infrastructure Developments (cont'd)

adoption.

The downside of all this is that vendors and customers still face major questions and risks as they choose their RFID infrastructure strategies. The upside is that great new ideas are still emerging and the industry is not prematurely locking into a suboptimal standard.

The Future of EPC Standards

In our opinion, two transitions are occurring: First, the transition from Savant to ALE represents a more advanced and powerful design for RFID infrastructure. An ALE based design acknowledges the importance of distributed networks. Second, the importance of EPC Global in driving RFID infrastructure is diminishing. This reflects the growing commercial influence in RFID and compelling RFID applications.

In general, these are positive developments. We like early-stage technology spaces to be commercially driven and not overly theoretical. The early EPC Global specifications have been very useful guideposts for the early RFID industry. They have also had significant flaws and the counterbalance of commercial innovation is helping to obviate these flaws. Throughout the remainder of this year, we expect commercial advances in RFID infrastructure to accelerate and continue becoming more important relative to the EPC Global standards. We also expect RFID to drive advances in massively distributed Internets with unprecedented numbers of nodes.

Going forward, we would like to see these new infrastructure advances applied more broadly. Today, particularly in North America, there is a dominant focus on passive RFID applied for tracking packages in Wal-Mart's supply chain. The basic concepts emerging in RFID infrastructure could be applied much more broadly to a wide variety of distributed network scenarios. This would include sensor networks, identity systems and mobile e-commerce platforms. There is a good opportunity for vendors in these spaces to embrace and extend the advances in passive RFID infrastructure thinking.

The RFID Spectrum

Many of us define our interest in RFID quite narrowly, limiting it to:

Passive RFID that operates at UHF frequencies around 900 MHz

Tags and tag numbering that comply with EPC Global standards

Supply chain applications where large packages are tagged and shipped to Wal-Mart or other major retail chains

By some measures there is a very large commercial opportunity defined within these limits. Vendors can sell and deploy vast infrastructure. Retailers, their suppliers and their distributors can save millions by improving visibility through RFID tagging.

Nevertheless, we try to view RFID applications and technology in much broader terms. We'd also like to see EPC standards efforts encompass this breadth. Various ISO standards for RFID encompass this breadth and include more advanced technology. We would like to see EPC leverage these efforts.

Classic Active RFID

Classic active RFID uses battery-powered tags that transmit a heartbeat periodically. In contrast, passive RFID tags only transmit when they are excited by the signal from a reader. Active RFID tags are tuned to generate the heartbeat efficiently, to extend battery life. The best active RFID tags can operate for about five years. The battery power also allows the tags to be read at a much longer distance than passive tags.

The RFID Spectrum (cont'd)

Companies to Watch Classic Active RFID

Baxter Healthcare
(http://quickfind.baxter.com)

Radianse
(http://www.radianse.com)

Savi Technologies
(http://www.savi.com)

Wavetrend
(http://www.wavetrend.co.uk)

WhereNet
(http://www.wherenet.com)

WiFi RFID

AeroScout
(http://www.aeroscout.com)

Ekahau
(http://www.ekahau.com)

Kidspotter
(http://www.kidspotter.com)

PanGo Networks
(http://www.pangonetworks.com)

Wavelink
(http://www.wavelink.com)

Some active RFID tags can be read from hundreds of meters away. Also, active RFID tags can operate better where there is electromagnetic interference and in the presence of liquids and metals. Such environments can be challenging for passive RFID. Active RFID tags and readers typically interact at UHF frequencies (most often 433 MHz).

Classic active RFID tags are more expensive. Generally, they cost between US$8.00 and US$20.00 per tag. Passive, EPC Class 1 tags are now available for less than 35 cents and the price continues to decline.

Active RFID is deployed widely in a variety of applications. Savi Technologies sells active RFID systems to governments and terminal operators. These systems are used to track vehicles and containers. WhereNet sells Real Time Location Systems (RTLS) that use active RFID for tracking trucks and automobiles in yards and distribution centers. Similar systems are also used for tracking moveable assets in hospitals and clinics. In this context, Baxter Healthcare's QuickFind system is a leading solution. In many factories, the trays, racks and totes have active RFID tags and these are used to indirectly track the products carried within them.

In general, reusable active RFID tags are used to manage vehicles, containers, assets and conveyance (with the understanding that these categories overlap). By contrast, many passive RFID applications are focused on using disposable tags to track products and packages.

Presence vs. Location

When tags and readers only operate at close range, presence determines location. In a typical 'Wal-Mart' deployment, a dock door is outfitted with readers. Any time a tagged package arrives and is read, its location is known by default.

With longer range RFID, this is not necessarily true. In a storage yard, an active RFID reader can detect everything within several hundred meters. This could include hundreds of vehicles. Beyond just presence, it is more valuable to know the precise location of the vehicle within the range of the reader.

To solve this problem, certain RTLS systems use Time Delay of Arrival (TDA) technology and other approaches exist as well. The time required for a signal to travel between an asset and a reader provides information about the distance from the asset to the reader. Multiple readers are deployed and the combined TDA information is used to accurately calculate the location of an asset. TDA-based systems can typically be used to locate objects with accuracy of 10 meters or less.

Also within this space, Radianse offers an Indoor Positioning System (IPS) to hospitals and clinics. Kidspotter sells systems that are used to locate lost children at amusement parks and ski resorts.

WiFi-Based RFID

WiFi is the wireless extension of the Internet based on the 802.11 IEEE standards. Today, virtually all laptop computers include WiFi-compatible radios. Recently, we purchased a printer with WiFi. Later this year, Wi-Fi-compatible telephones will start becoming available. WiFi has many customers and vendors. The ongoing investment in WiFi technology and deployment is massive.

Resulting from this investment, the cost of WiFi radios continues to decline. Within the past three years, WiFi-based active RFID tags have emerged. Now they are becoming cost-competitive with classic active RFID. Since WiFi-based tags offer comparable performance, range and price, we expect WiFi-based RFID to continue strengthening in the coming two years.

Resulting from widespread adoption, many RFID deployment sites already have WiFi networks installed. WiFi-based RFID can use these existing networks but classic RFID

The RFID Spectrum (contd.)

requires deployment of new networks of readers. Consequently WiFi can have a big cost advantage over classic RFID.

Since WiFi is simply an extension of the Internet, all WiFi-compatible tags and readers are uniquely identified. Each 'node' has a 48-bit Media Access Control (MAC) address. With 250 trillion possible MAC addresses, we wonder why there is a need for any other unique numbering system in the world. Rather than struggle between EPC, UID, GUID, NDC and GTIN, all objects could be numbered with MAC addresses or MAC addressing's 64-bit EUI extension. These objects would be uniquely numbered and Internet-compatible at the same time.

Aeroscout is a leading vendor of WiFi-based RFID systems. Other leading players include Wavelink, Ekahau and PanGo Networks.

Presence vs. Sense

When tags – such as EPC class 1 tags – only store a single unique number, they can only report their presence at a given location. Classic active RFID tags often provide environmental sensors as well. For example, an active tag monitoring the bearings in rail car wheels can report the temperature of the bearings as the car rolls by a reader. Elevated temperature indicates wear and the tag can be used to trigger maintenance before bearing failure causes a derailment.

Classic and WiFi-based RFID tags can also provide links to the computing devices in which they are embedded. Tags that are used to track the moveable equipment in a hospital or clinic can provide telemetry – reporting the effectiveness, configuration and duty cycle information of their host devices.

Since these tags are essentially computing devices themselves, they can also implement security and authentication policies. As the quantity and importance of information reported from tags increases, these tags can ensure that information is protected and only shared with authentic clients.

These capabilities are all building blocks of highly distributed sensor networks based on RFID.

Other Wireless Technologies

WiFi-based RFID is a competitive alternative to classic active RFID that has significant advantages. In our effort to understand the RFID spectrum, we have been investigating other wireless technologies that are sometimes considered for RFID.

Bluetooth beats WiFi in both cost and power consumption. It also has fast data transfer and adequate security. Today, Bluetooth is mainly used for wireless headsets transmitting voice. Bluetooth lacks the networking and addressing capability that is required for managing many devices in a network simultaneously. Bluetooth is essentially a short-range cable replacement that can link 8 devices together. Bluetooth is a mature standard and widely used with more deployed devices than WiFi.

Ultra Wide Band (UWB) is a potential successor to Bluetooth offering faster data transfer and even lower power consumption. UWB's data transfer rate is roughly equivalent to Universal Serial Bus (USB) 2.0. The first popular UWB-based product will likely be a wireless USB hub that allows personal computers to wirelessly connect with peripherals.

Unfortunately the UWB standardization effort has recently become fragmented between rival proposals from Intel and Motorola. We don't expect USB to begin supplanting Bluetooth for at least three years.

Zigbee is another emerging technology that could be very well suited for RFID in the future. Zigbee offers low cost and power consumption. It does not offer fast data transfer, but it does have extensive networking and addressing capability. This makes it very well-suited for linking up large

The RFID Spectrum (contd.)

collections of objects and sharing modest amounts of information from each.

Bluetooth, UWB and Zigbee are all based on variants of the 802.15 IEEE standards.

Is Privacy Possible With RFID?

When EPC Global and its followers decided to back away from item-level tagging in 2003, a thorny issue was diffused. Privacy advocates were voicing concern that consumers could be tracked by the tagged items they purchased and carried. Despite the fact that tagged consumer products are still at least five years away, we are seeing several emerging scenarios where people will end up carrying tagged items that could allow them to be tracked and their privacy compromised. Prominent examples include:

Toll-paying devices attached to cars can be used to track their movement and in turn, the movement of the driver and passengers.

Public transit passes can be used to record where and when individuals enter and exit urban transportation systems.

Extensions of transit passes and independent new systems are allowing individuals to make purchases and other transactions with tags.

Machine-readable travel documents such as passports can be used to track individual movement around airports and other travel-related locations.

Libraries are tagging books and other materials, which is a precursor to item level tagging in stores.

With the spread of these and other applications, increasing numbers of people are carrying tags wherever they go. The issue of adequately guaranteeing personal privacy is becoming more important. This is a complex issue that involves technology, public policy and the rights of individuals.

At RFID-World on March 2 in Dallas, we are presenting the session entitled, “Security, Authentication, Privacy and Trust”. The session will cover the technology of security and authentication as well as the issues of privacy and trust.

Security & Authentication

Modern methods of providing security in the digital world rely on cryptographic protocols requiring significant computing power. The sophisticated tags used in Smartcards have this power and are capable of securing transactions. EPC will not have sufficient power to support cryptography for at least several years.

A key element in secure communication is proper authentication of the parties involved. This enables both sides of a secure communication to trust the true identity of each other, preventing unwanted communication with rogue parties. Unfortunately, reasonable authentication requires cryptographic power. Although the EPC Class 1 tag specification requires password access to its kill command, the password implementation is weak and does not guard against general access to the tag.

The lack of cryptographic power in EPC tags has led various parties to propose solutions that degrade tag functioning rather than securing it. A “blocker tag” can be introduced near valid tags to prevent them from being read. The blocker tag broadcasts a big set of tag ids, confusing any reader within range. Obscuring bags and cases have also been proposed. Consumers could carry their tags in these containers when they don’t want the tags to be read.

Defenders of RFID often cite short read range and the inability to read tags in certain environments. It is true that EPC tags can only be read from a short distance by a

Is Privacy Possible with RFID? (cont'd.)

Groups to Watch Privacy Standards

Platform for Privacy Preferences (P3P) Project
http://www.w3.org/P3P/

Enterprise Privacy Authorization Language
http://www.w3.org/2003/p3p-ws/pp/ibm3.html

Privacy Advocates

American Civil Liberties Union (ACLU)
http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=15559&c=207

Electronic Freedom Foundation (EFF)
http://www.eff.org/Privacy/Surveillance/RFID/

Electronic Privacy Information Center (EPIC)
http://www.epic.org/privacy/rfid/

Simson Garfinkel
http://www.technologyreview.com/articles/garfinkel1002.asp

legally compliant, standard reader. The problem is that rogue, illegal readers can be constructed by boosting signal power and adding creative algorithms based on anti-collision. These readers are more sensitive and can learn about tags from further distances and in challenging environments. It is also possible to connect such a reader to a camera and capture an image of any person carrying a tag as they come within range. As more people carry tags, the problem of unwanted identification will become more widespread.

Privacy & Trust

The lack of security and authentication in low-cost tags hinders the ability to guarantee secure RFID transactions. Therefore, protecting a person's rights for information disclosure will depend primarily on business practices and public policy.

In the U.S., the policy side will be driven by the protections built into the First and Fourth Amendments of the Constitution. These policies appear in various laws, such as the Cable Television Privacy Act, the Video Privacy Protection Act, and numerous other laws and legal opinions stemming from the tenets of Fair Information Practices. Although such laws can protect access and usage of the databases behind RFID implementations, they do nothing about rogue reads of tags.

In order to avoid cumbersome and excessive legislation of privacy and yet establish trust with consumers, many businesses are adopting privacy policies that explicitly declare how personal information will and will not be used. Auditable enforcement of such privacy policies is being development by encoding the contract of a policy in a privacy specification language, such as P3P and EPAL (both part of the World Wide Web Consortium standards body). These developments are still in the early stages, so their impact and effectiveness are not yet known.

Lastly, numerous individuals and groups, including the American Civil Liberties Union (ACLU) and Electronic Frontier Foundation (EFF), are advocating the establishment of rights for consumers with regard to RFID as part of a larger campaign advocating consumer rights and freedoms in an increasingly digital world. Simson Garfinkel's RFID Bill of Rights, published in MIT's *Technology Review*, best articulates adapting fair use practices to RFID. His rights for the consumer include:

- Know which items have tags
- Can remove/deactivate tags after purchase
- Can access data associated with tags
- Can access services without requiring tag
- Know when, where, why of data usage

Conclusions

With emerging technologies such as RFID, widely adopted standards provide certainty and reduce the risk associated with investment. In passive RFID, we continue to see dual progress from the EPC specifications and de facto commercial initiatives. Specifically the EPC numbering standard is well-understood but not yet widely used. We expect and hope it will be challenged by more sensible de facto alternatives such as Internet numbering. ALE provides improved guidance for the development of RFID infrastructure but de facto alternatives are gaining traction as well. Commercial advances in readers, routers, edge servers and enterprise middleware are implementing some of ALE's good ideas today. At the same time, these advances

Conclusions (contd.)

from established players are creating uncertainty for pure play RFID middleware and infrastructure vendors.

No similar broad standards are being promoted for active RFID. We would like to see active RFID players adopt some of the same infrastructure standards emerging in the passive realm. These standards are applicable. This would cement the idea that active RFID tags are just another type of network edge sensor, with similar network requirements to passive RFID. Active RFID is benefiting from advances in the standards of adjacent technologies such as WiFi and the various 802.15 standards including Bluetooth, UWB and Zigbee.

Active RFID is gaining traction today because it is being applied in stand-alone solutions with clear ROI and few hindrances. Enterprises are using active RFID internally to track assets, people and conveyance. The resulting increase in efficiency and reduction in losses are easy to identify. Generally speaking, these applications don't require unprecedented collaboration and they don't create new personal privacy issues. More complex tags and better radios will make these applications even more appealing in the future.

Passive RFID is still locked within mandates, pilots and trials. Compliance, rather than clear ROI, is driving many deployments. The 'Wal-Mart' vision for RFID will not be fully realized until the cost of tags, readers and deployment are reduced significantly from today's levels. Also, the vision requires unprecedented collaboration and information sharing between Wal-Mart and its suppliers. It's nearly impossible to predict when and how that will happen.

Privacy concerns continue to inhibit certain large scale RFID deployments. The issue was diffused somewhat when the EPC players backed away from item-level tagging in late 2003. Nevertheless, privacy is a major concern with digital identity and e-commerce applications of RFID. We would like to see these concerns resolved two ways. First, existing technology can be applied to implement better security and authentication in RFID tags. Second, policies for fair use of information should be expanded and respected. With a combination of technology and policy, certain RFID applications will become more acceptable to consumers. This issue will never – and should never – be considered resolved. Consumers should always be diligent and certain identity applications should always be resisted.

About Big Chief Partners

Big Chief Partners offers strategic advice, research and software development for organizations that want to capitalize on identification technologies, mobile payments, infrastructure, security and RFID.

The Partners are Peter Winer, Alice Lankester and Chris Meisl. We are experienced software entrepreneurs, developers and company managers. Each of us has between 15 and 20 years of software industry experience with a large number of startups and well-known global enterprises. We also tap into a broader network of experts who further increase our depth within specific technologies and markets.

Starting early 2001, Big Chief Partners first involvement with RFID was developing the WebLink system for Philips Semiconductors. Since that time, we have provided implementation and advice for numerous other companies investing in RFID. We have also published newsletters and contributed in many RFID conferences.

Clients include technology vendors, customers pursuing RFID deployment, conference organizations and venture investors in the U.S. and Europe.

Subscriptions

This newsletter is distributed as a service to individuals and organizations having a business relationship with Big Chief Partners. This newsletter is not widely distributed, and is only sent to people who wish to receive it. If you have colleagues or business partners who might benefit from receiving the newsletter, please let us know.

To subscribe to this newsletter, send an email to info@bigchief.com. To unsubscribe, send an email to info@bigchief.com with “unsubscribe” in the subject line.

Back issues of newsletters, presentations from conferences and other content are available on the Big Chief Partners Web site at http://www.bigchief.com/whitepapers.

To subscribe to this newsletter, send an email to info@bigchief.com.

Contact Us

Big Chief Partners, Inc.

Los Altos, CA 94022 USA

Voice: **(650) 917-3833**

Fax: **(650) 917-3831**

Mail: **info@bigchief.com**

Web: **http://www.bigchief.com**

Blog: **http://www.bigchief.com/weblog**